Wireless Use Case Analysis

This document steps through a list of wireless uses cases that are relevant to scope of the VVSG requirements. Each use case is followed by concerns, suggested mitigations and related requirements.

Peripheral input/output devices such as a keyboard, mouse, headset, or printer

Peripheral devices can communicate over wireless technology to input and output data from the voting system. These devices are portable and allow for cross device compatibility. Input devices such as a keyboard or mouse may connect over Bluetooth and allow election workers to type and navigate when interacting with the voting system. Output devices such as a Bluetooth headset or printer may be used to wirelessly review and print a ballot on a ballot marking device.

To print Ballots on Demand, multiple laptops may wireless print to a single printer in vote center.

Concerns

Loss of availability to perform election functions and access election data

- Denial of Service (DoS) via Jamming - Radio jamming can cause disruption or interference with the transmission of data. This impacts availability by preventing the input and output of data to and from the peripheral devices. This can halt functionality in the polling place if election workers/voters are not able to input data into the voting system or output data such as, printing a voter's ballot selections.

Loss of confidentiality and integrity of election data

- Machine-In-The-Middle (MITM) Attack - The information sent wirelessly may be susceptible to a MITM attack. This could allow an attacker to eavesdrop or maliciously modify the data in transit. This impacts the confidentiality of the election information if unauthorized users are able to access election data and impacts the integrity if attackers are able to modify election data (e.g., tabulation totals).

- Remote Malware Injection - Wireless technology may provide entry points for attackers to access or harm the voting system. If an attacker gains access to the voting system through wireless technology, they may be able to remotely inject malware or modify files within the voting system. This impacts the integrity of the information on the voting system if the malware is able to modify files such as, maliciously tampering with tabulation results or deleting ballot records. The confidentiality of the information on the voting system is impacted if the malware is used to reconfigure the wireless technology to send data to an unauthorized receiver.

Loss of ballot secrecy

- Logging Device Information – When wireless devices connect to the voting system, information about that connection is logged. This may include the type of device, the device owner, and the time that device was used. The concern here is that this information is retained in the voting system and may allow the logged device information to be used to link a voter to their ballot selections.

Potential Mitigations

No Bluetooth hardware

The voting system does not contain any Bluetooth hardware and only allows for physical connections to peripheral devices.

Disable Bluetooth

Turn off Bluetooth interface so that it cannot be used or is only used when necessary. This may be done manually or automated based on the voting state (e.g., activated state).

Sophisticated security awareness and secure configuration management

Bluetooth devices often do not receive updates once deployed. To ensure the device has the latest security capabilities, the device should be using the latest version of the Bluetooth protocol. The Bluetooth device should also implement the highest security configurations for encryption, authentication, and data signing. Additionally, to maintain the security of the wireless technology, there should be a process to review and update the technology.

This requires election workers to be aware of the Bluetooth specs for their own personal devices that they bring into the polling place. The technical expertise of election workers varies. To properly ensure this mitigation is applied it may require additional technical staff to be present at each polling place.

Ballot Activation Card

A voter is given an activation card. This card may use near-field communication (NFC) and either is inserted or held near a voting device to activate a voter's ballot with the appropriate ballot style.

Concerns

Loss of ballot secrecy

- E-pollbook Data Transfer - If the activation card receives the ballot style configuration from an e-pollbook, voter identifying information may be stored and transferred onto the activation card and then to the voting system. With this information now inside the voting system, it could be used to link a voter to their ballot selections.

Loss of integrity of activation card information

- Modification of Activation Card - An attacker may insert an activation card into their own malicious device to modify the information on the activation card. This impacts the integrity of the information transmitted and presented on the voting device. For

example, a voter may be provided with the wrong ballot style, which could then impact the accuracy of their vote selections.

- Malware Injection - A malicious actor may use the activation card to inject malware into the voting device. This could impact the integrity of the voter's input and the output of their ballot selections. One example is the malware could be used to ignore the voter's input and only input votes for one specific candidate without the voter's awareness.

Potential Mitigations

No NFC Hardware

The voting system does not contain any NFC hardware and must use an alternative method to activate a voter's ballot.

Disable NFC

Turn off NFC interface so that it cannot be used or is only used when necessary. NFC chips do not function unless activated. This can assist in preventing accidental and malicious attempts to transmit data.

Sophisticated and ongoing methods for secure configuration management and implementation

Unlike Bluetooth and WiFi, NFC devices do not have a sophisticated pairing process. NFC devices can talk to any other device that is NFC capable. Any security capabilities could be done at the application layer. The voting device would require credentials to authenticate and verify an authorized activation card. Also, digital signing could be used to verify the information on the activation card was not modified. Additionally, to maintain the security of the wireless technology, there should be a process to review and update the technology.

The technical expertise of election workers varies. To properly ensure this mitigation is applied it may require additional technical staff to be present at each polling place.

Manage Local Devices

An EMS is equipped with WiFi to wirelessly provide device level management to devices in the polling place. This may include sending device configurations or updates.

Concerns

Loss of availability to perform election functions and access election data

- Denial of Service (DoS) - Radio jamming can cause disruption or interference with the transmission of data. This impacts availability by preventing the EMS from managing the devices within the polling place and transfer the appropriate information the those devices.

Loss of confidentiality or integrity

- Machine-In-The-Middle (MITM) - The information sent wirelessly may be susceptible to a MITM attack. This could allow an attacker to eavesdrop or maliciously modify the data in transit. This impacts the confidentiality and integrity of the information transferred.

- Remote Malware Injection - Wireless technology may provide entry points for attackers to access or harm the voting system. If an attacker gains access to the voting system through wireless technology, they may be able to remotely inject malware or modify files within the voting system.

Potential Mitigations

No WiFi Hardware

The voting system does not contain any wireless hardware. This may require manually managing and configuring each device.

Disable WiFi

Turn off the WiFi interface so that it cannot be used or is only used when necessary. This limits constant broadcasting and can assist in preventing accidental and malicious attempts to transmit data.

Sophisticated and ongoing methods for secure configuration management and implementation

Ensure that strong encryption and authentication is applied in your WiFi implementation. This requires using the latest WiFi security protocols (WPA2/WPA3) and proper configuration within your network.

The technical expertise of election workers varies. To properly ensure this mitigation is applied it may require additional technical staff to be present at each polling place.

Transmission of Election Results

Elections results are transferred to the central tabulation center over cellular. This technique is often used for rapid reporting of unofficial election results. Additionally, this method is used in geographical areas or conditions that may make it challenging to transport election data between precincts and central count centers (e.g., mountainous or rural areas).

Concerns

Loss of availability to perform election functions and access election data

- Denial of Service (DoS) - Radio jamming can cause disruption or interference with the transmission of data. This impacts availability by preventing the transfer and access to election data. In this scenario, central count centers would not be able to receive election results from their local precincts and would have to use an alternative method to obtain the election data to perform election night reporting of election results.

Loss of confidentiality and integrity of the voting system

- Extensive Remote Access to the Voting System – Cellular expands the attack surface even further because the data traverses over the internet, which itself touches all over the globe. Exposure to the internet could enable nation-state attackers in other countries to gain remote access to the voting system. With remote access an attacker

can view all files within a voting system and make modification to files within the voting system. These files may include, election results.

- Remote Malware Injection - Exposure to the internet may also enable nation-state attackers to remotely inject malware that maliciously modifies or deletes files within the voting system. Malware injected into the central count system could impact the integrity of the election results received from all precincts within a State. The malware may also be used to reroute information from the voting system to the computer of a nation-state attacker.

- Machine-In-The-Middle (MITM) - The information sent wirelessly may be susceptible to a MITM attack. This could allow an attacker to eavesdrop or maliciously modify the data in transit. This impacts the integrity of the data because an attacker may be able to view and modify the election results prior to the data reaching the central tabulation center. This could result in an inaccurate report of the elections results.

Potential Mitigations

No Cellular Capability in the voting system

Voting systems would not have a cellular transmission capability within their architecture. Alternatively, elections results could be transmitted through other methods including…

- The manual sneaker-net process, where the data is transferred via USB/printed results, and sent to the central tabulation center
- Telephone communication to send election results via a phone call or text message
- Using a mobile application to send election results to the central tabulation center

Airgap at Both Ends of Communication

Ensure that the device that sends the elections results is kept separate from the rest of the voting system. Additionally, at the central tabulation center, the receiving device would be kept separate from the machine that performs the final tabulation. Information must be manually transferred from the tabulation system to the election reporting machine. This protects the information on the voting system from malicious tampering.

Airgap + Sophisticated implementation of a secure transmission

This requires secure configuration and implementation. The voting system would use methods to keep communications private, such as using a trusted virtual private network (VPN) to encrypt the data and traffic. This does not prevent a user from downloading malware from the internet but protects the confidentiality of the data sent. Another method is to use secure file transfer tools that encrypt the data in transit and sends to authorized recipients.

Related Principles and Guidelines

Guideline 2.5: "The voting system supports system processes and data with integrity." Requirements that cover I/O integrity, such as detecting errors, validating input, and sanitizing output, all have implications in the discussion of wireless technology. As network connections provide a means of input and output, the same principles that require validation and security around simple I/O devices should apply to network input and output as well, at all layers of the network stack.

Guideline 2.6: "The voting system handles errors robustly and gracefully recovers from failure." In particular, the requirement "System must survive device failure" is very important for any system that uses wireless technologies.

Guideline 10.2: "The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections." Any information wireless transmitted to the voting system should not include any voter identifying information.

Guideline 12.1: "The voting system supports mechanisms to detect unauthorized physical access." Applies to wired network connections, which could be physically connected or disconnected.

Guideline 12.2: "The voting system only exposes physical ports and access points that are essential to voting operations." Applies to ports and interfaces used for network connections, which should not be exposed if present on a device.

Principle 13: Data Protection. This principle and its requirements apply directly to any data carried over a network connection.

Guideline 14.2: "The voting system limits its attack surface by reducing unnecessary code, data paths, physical ports, and by using other technical controls." Network connections constitute a significant attack surface that should be reduced as strictly as possible.

Guideline 15.1: "Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing." Section 15.1-E details system events that should be logged including networking events.

Guideline 15.4: "A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice." This guideline relates directly as it focuses on best practices for securing systems with network capabilities.